Advances in Intelligent Platform Management: Introducing the New IPMI v2.0 Specifications

Tom Slaight
Principal Server Management Architect
Intel Corporation

February 18, 2004

Special Guests!

Phil Chidester

Manageability Architect

Server Management Firmware Group

Dell Computer

Steve Lyle

Manageability Architect

Hardware Systems Technology Division

Hewlett-Packard Company

Agenda

- IPMI Architecture and Initiative Update
- What's New in IPMI v2.0?
- IPMI v2.0 Technology: How it meets platform management needs
- IPMI in Action
- IPMI Futures

IPMI

Intelligent Platform Management Interface

- **Defines a standardized, abstracted, message-based interface to intelligent platform management hardware**
- **Defines standardized records for describing platform management devices and their characteristics**

Promoters: Intel, Hewlett-Packard, NEC, Dell

Adopters: 162 and growing

IPMI Enables Cross-Platform Management Software

Initiative News

IPMI v2.0 Specifications
Updated v1.5 Errata, 32- and 64-bit Drivers,
& IPMI Conformance Test Suite

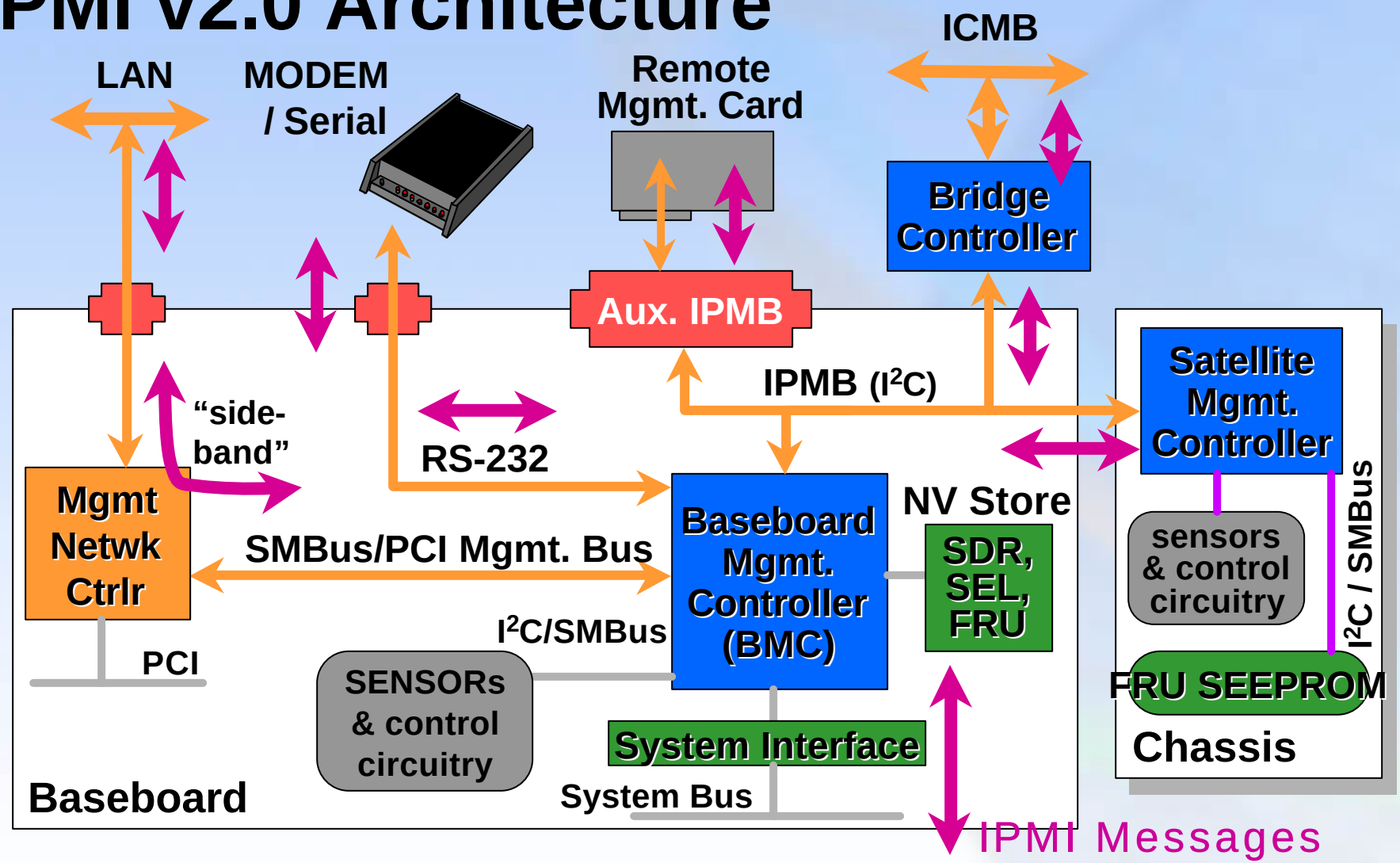
developer.intel.com/design/servers/ipmi

New Adopter's Agreement

- **IPMI v2.0 Second Generation Specification is under RAND (Reasonable And Non-Discriminatory) licensing model**
  - Aligns with Industry standards licensing models (e.g. DMTF*, PICMG*, Infiniband*, etc.)
- **All companies (including existing IPMI 1.5 adopters) will need to sign new IPMI v2.0 adopters agreement to implement IPMI v2.0 spec**
  - Existing IPMI 1.5 adopters can continue to implement IPMI v1.5 under old licensing terms, but to new IPMI v2.0 agreement required to implement new IPMI v2.0 features
- **New IPMI v2.0 Adopters license available on IPMI web site for your review**

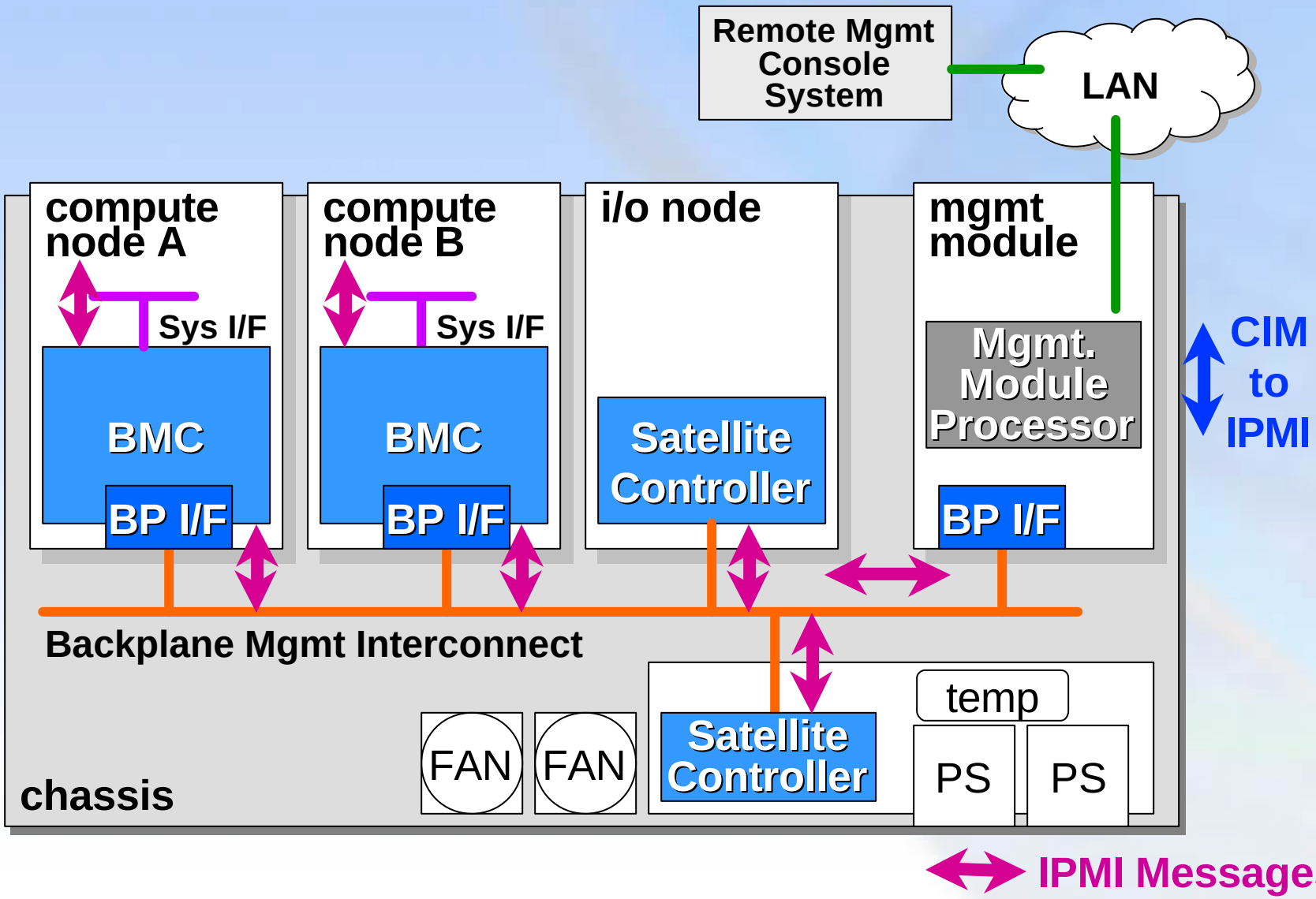
Sign Up as IPMI 2.0 Adopter Today!

IPMI v2.0 Architecture

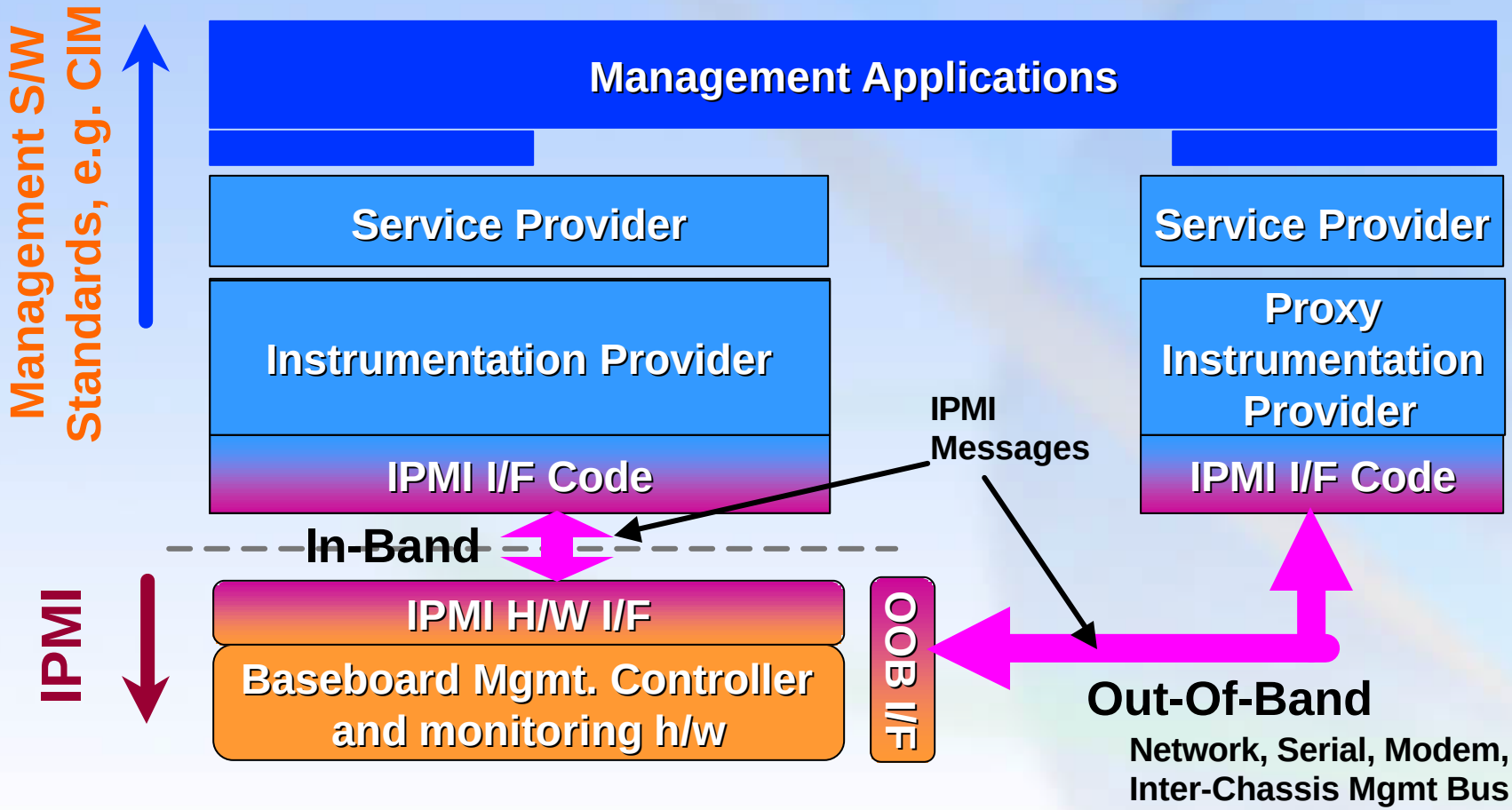


IPMI in modular architecture

Typical Modular Application



Where it fits…



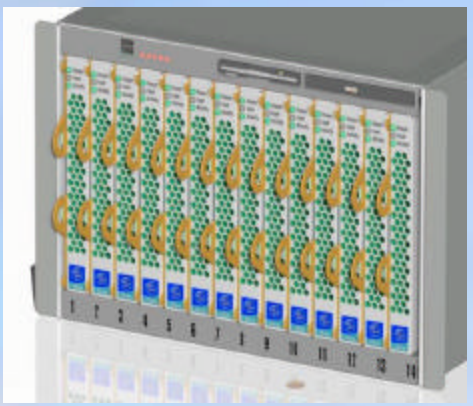
IPMI helps reduce TTM and development cost for cross-platform management

Agenda

- IPMI Architecture and Initiative Update
- What's New in IPMI v2.0?
- IPMI v2.0 Technology: How it meets platform management needs
- IPMI in Action
- IPMI Futures

Platform Directions for IPMI

- Integrated 'Serial over LAN' management
- Low Cost Systems
  - "Baseline" BMCs
- Group Managed Systems
  - ICMB and LAN-managed systems
- Modular Systems
  - General purpose and Service Availability Forum "AdvancedTCA" blade systems



IPMI enables competitive features across server classes

IPMI v2.0 Additions

- Serial Over LAN (SOL)
  - Redirects local serial interface over an IPMI Session
  - Works with serial-based OS ‘command line’ interfaces
- LAN Session Enhancements
  - New user login and security configuration options enable tailoring security and performance to match the needs of the site
  - “Payloads” capability enables multiple types of management traffic (e.g. IPMI and SOL) over a single LAN session
- Enhanced Authentication
  - Stronger key exchange uses two-way challenge/response
  - Aligns with DMTF ASF 2.0* session establishment
- Packet Data Encryption
  - Enables remote operations such as user password configuration
- VLAN Support
  - Facilitates setting up ‘management-only’ networks

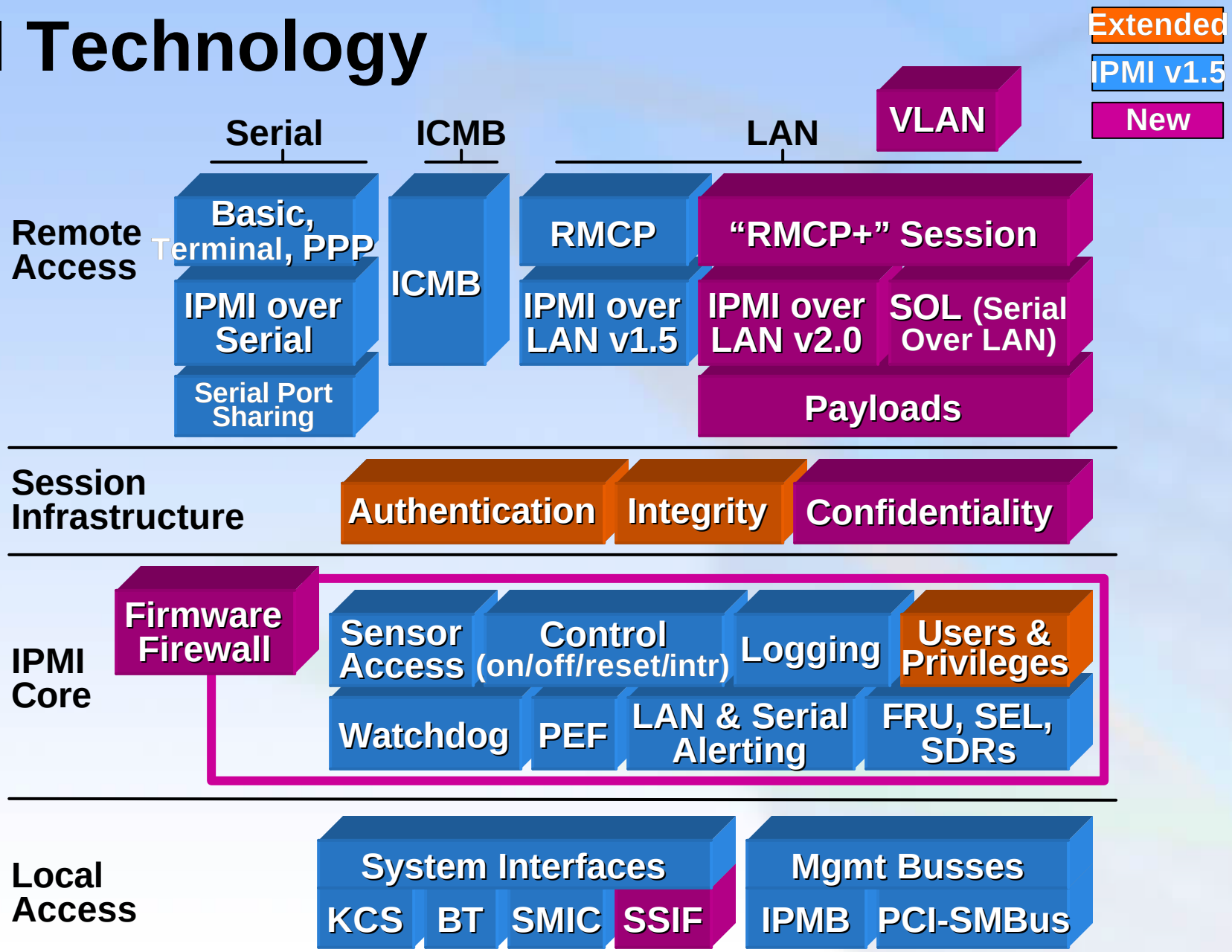
IPMI v2.0 Additions

- **Low-cost BMC Support**
  - **SMBus System Interface (SSIF) provides low-pin count system interface for low-cost (low pin-count) BMCs**
- **Modular Extensions**
  - **Node replacement, Redundant Management Bus monitoring, "Firmware Firewall" tailor IPMI to better support blade implementations**
- **Enhanced OEM value-added feature support**
  - **Support for OEM Security Algorithms and Payload options (e.g. KVM) on IPMI infrastructure**

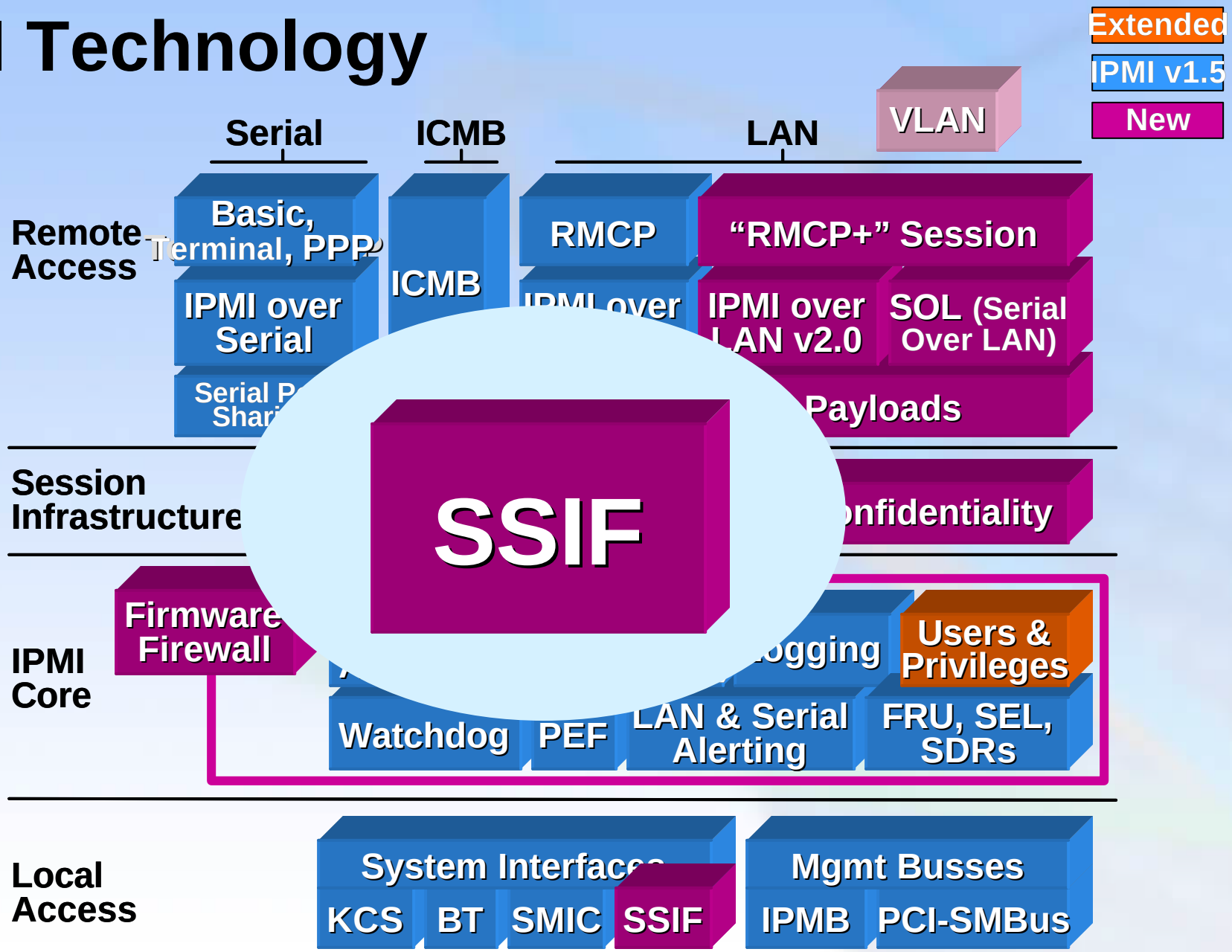
Agenda

- IPMI Architecture and Initiative Update
- What's New in IPMI v2.0?
- IPMI v2.0 Technology: How IPMI v2.0 meets platform management needs
- IPMI in Action
- IPMI Futures

IPMI Technology



IPMI Technology



SMBus System Interface (SSIF)

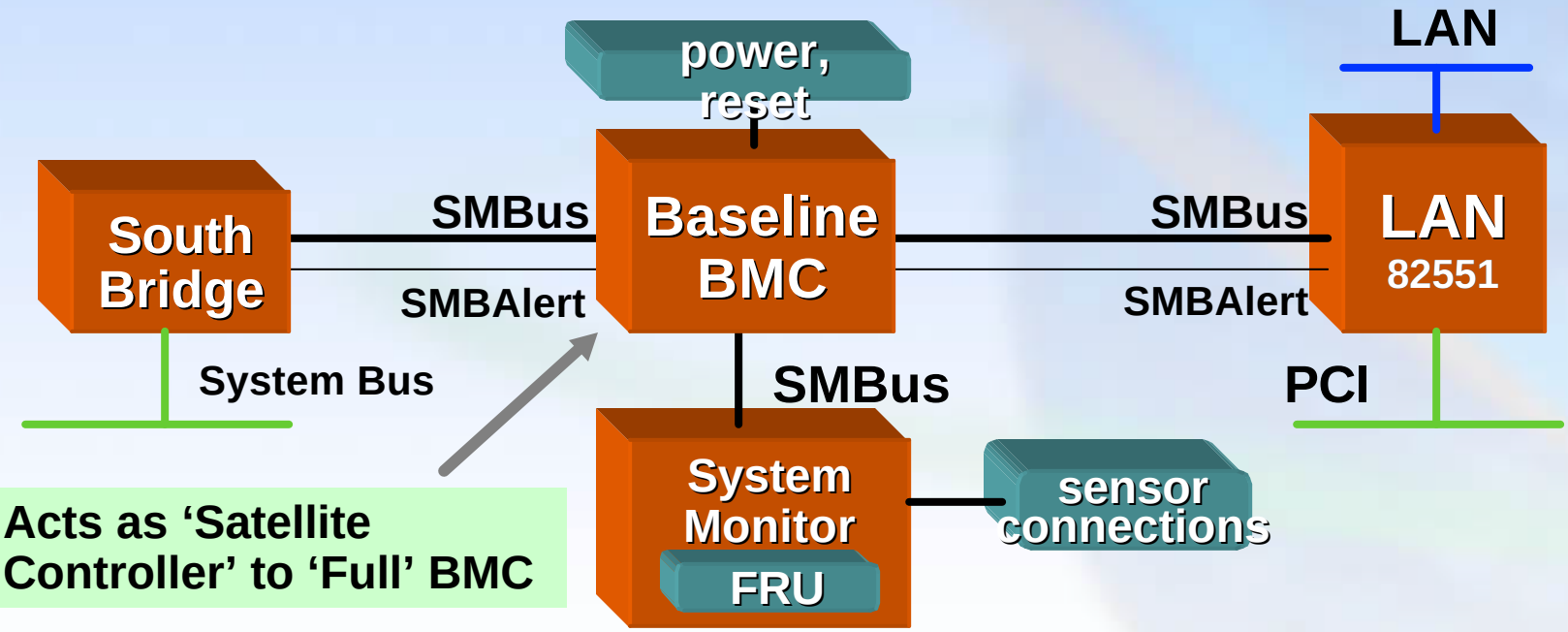
- Encapsulates IPMI messages in an SMBus compatible format
  - Compatible with common SMBus Host controllers
  - IPMI Requests delivered using ‘Block Write’ protocol
  - IPMI Responses retrieved using ‘Block Read’ protocol
    - SMBAlert signal status change/message available
- SMBAlert line notifies host that incoming message / status data is available
    - ‘Get Status’ command allows interface status to be polled

SMBus System Interface (SSIF)

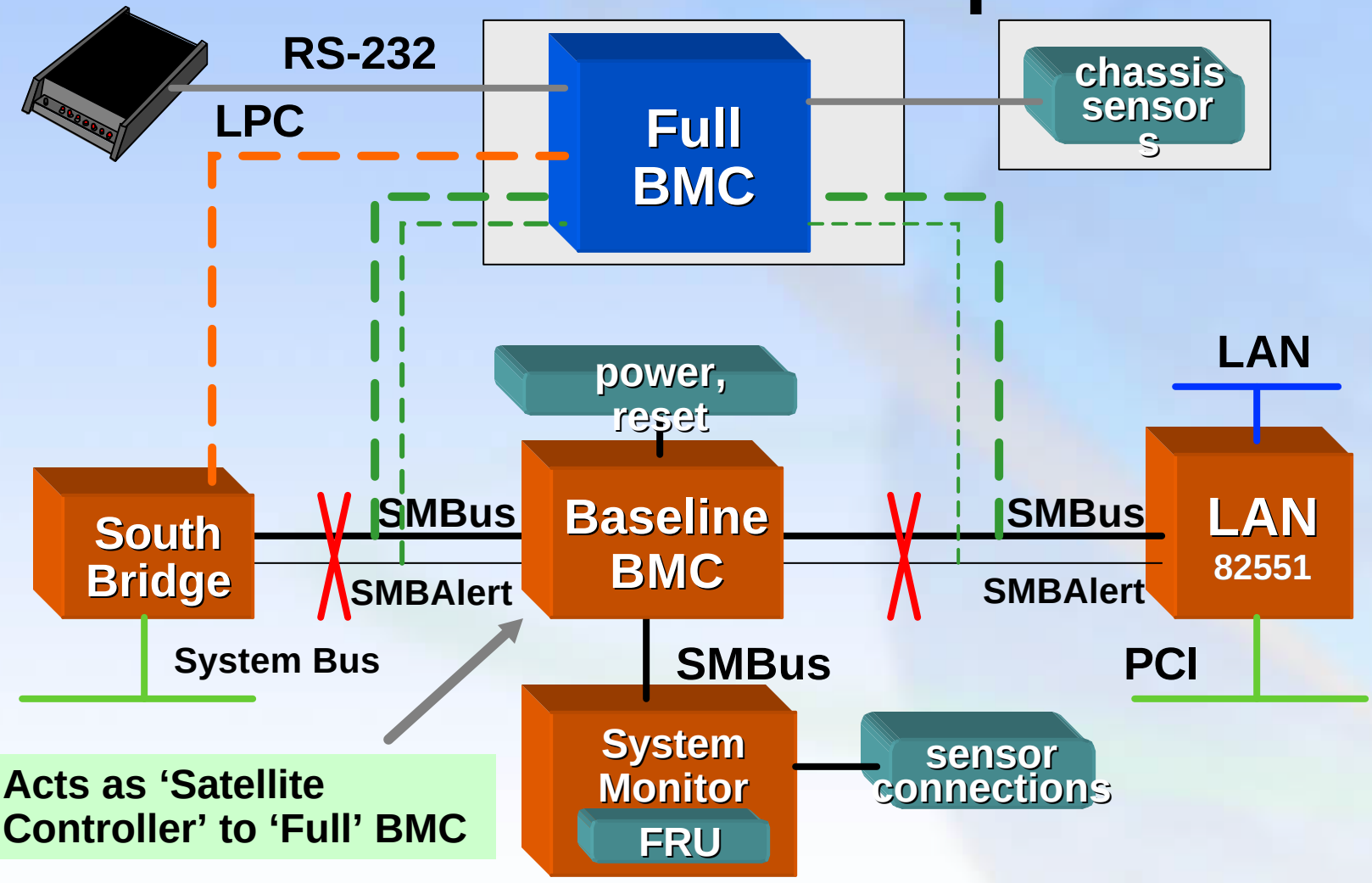
Local (System Interface) Discovery

- BIOS tables describe location and type of system interface
  - New ACPI “SPMI” (service processor mgmt. interface) Table
  - SMBIOS Type 38 Record
- SPMI and Type 38 Tables Applicable to *all* IPMI System Interfaces
  - SMIC, KCS, BT, SSIF

SSIF and Multi-level BMC Options



SSIF and Multi-level BMC Options



Low Cost Options enable IPMI for all Server classes

SMBus System Interface (SSIF)

Single Part Messages

- Used for IPMI Message Content up to 32 bytes (SMBus protocols limited to 32-bytes of data)

BMC Write / Request
(via SMBus Block Write)

WR
- BMC Slave Addr. | Wr
- SMBus CMD = *0x02*
- Length
  - IPMI NetFn (even) | LUN
  - IPMI Command
  - <IPMI Command Data>

BMC Read / Response
(via SMBus Block Read)

WR
- BMC Slave Addr. | Wr.
- SMBus CMD = *0x03*
- BMC Slave Address | Rd.

RD
- Length
  - IPMI NetFn (odd) | LUN
  - IPMI Command
  - IPMI Completion Code
  - <IPMI Command Data>

IPMI Message Content

SMBus System Interface (SSIF)

Multi-part Messages

- **Used for IPMI Message Content >32 bytes**
- **Block numbers enable retrieving lost or corrupted middle or 'end' read data**

BMC Multi-part Write / Request

(follows single part format for Start, but uses special SMBus CMDs for start and transferring remaining data)

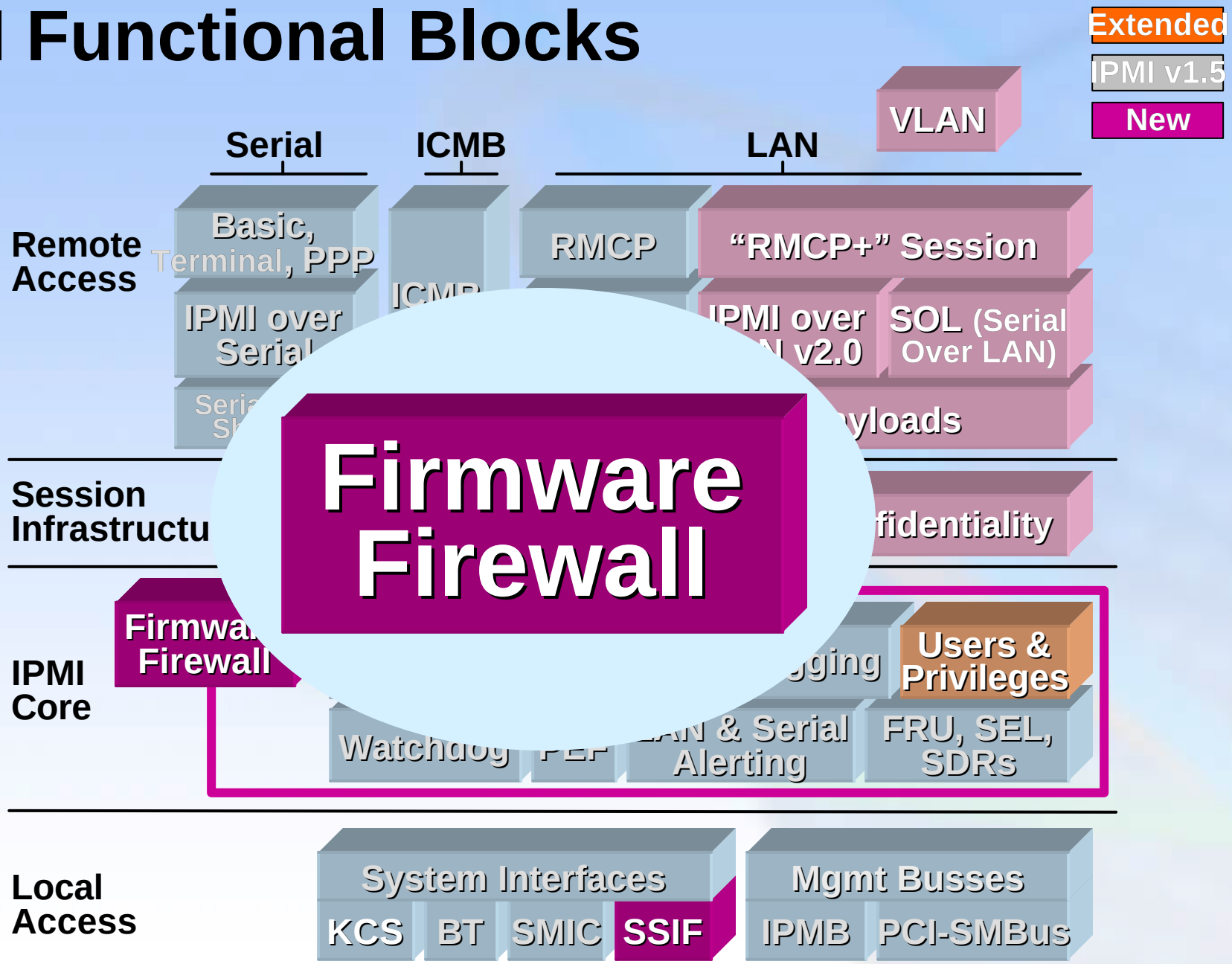
- **Start: SMBus CMD = 0x06, remainder matches single part format**
- **Middle: SMBus CMD = 0x07, followed by add'l request data**
- **End: SMBus CMD = 0x08, followed by last part of data**

BMC Multi-part Read / Response

(Starts off with reserved pattern [0x01, 0x00] then uses special SMBus commands to retrieve remaining data)

- **Start: SMBus CMD = 0x03, followed by [0x01, 0x00] then regular response data (NetFn | LUN, CMD, etc.)**
- **Middle: SMBus CMD = *0x09*, First byte = 00b followed by add'l response data**
- **End: SMBus CMD = *0x09*, First byte = 01b, followed by last part of data**

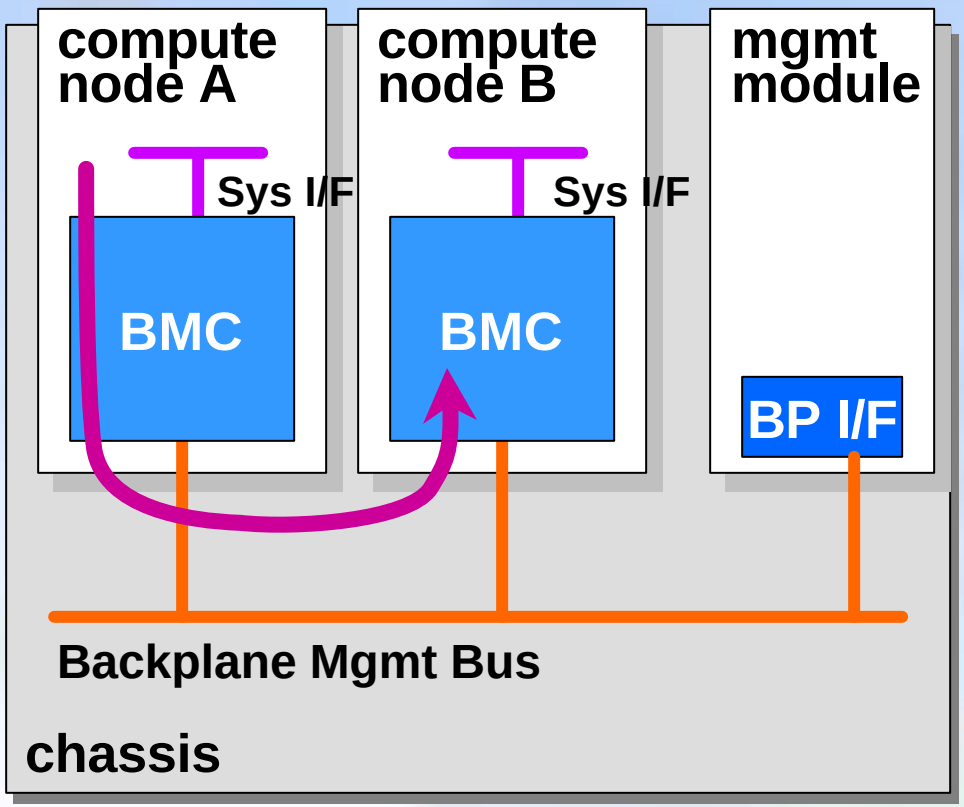
IPMI Functional Blocks



Firmware Firewall

Partitioning for protection

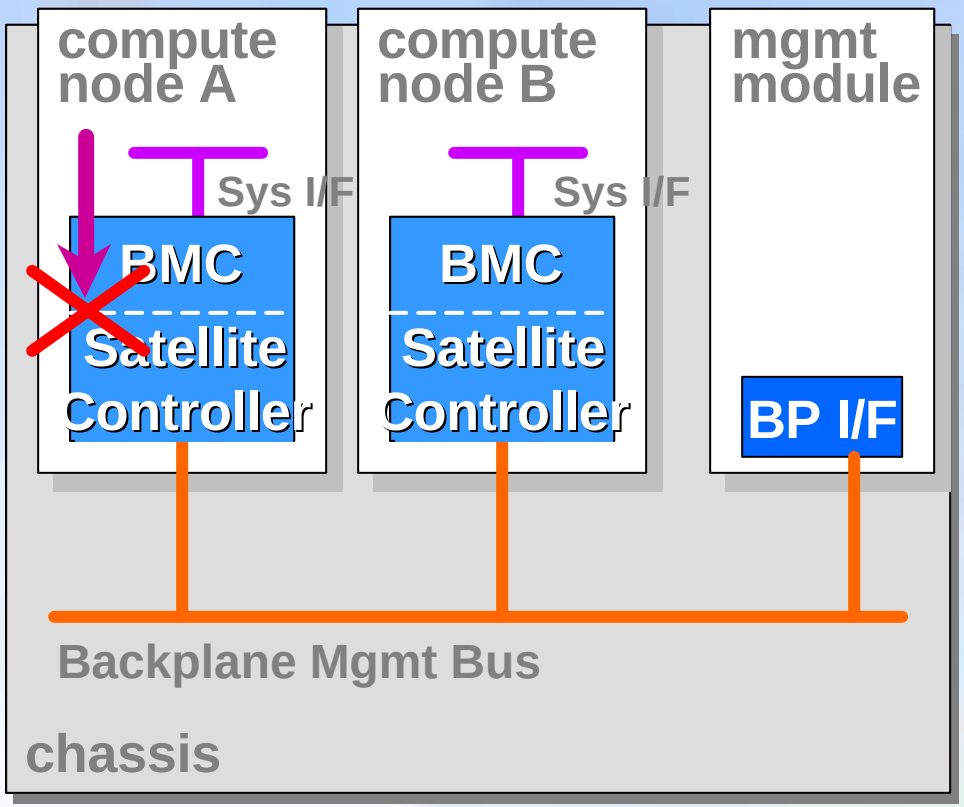
- **Problem: Bus topology enables local mgmt s/w to access other nodes**



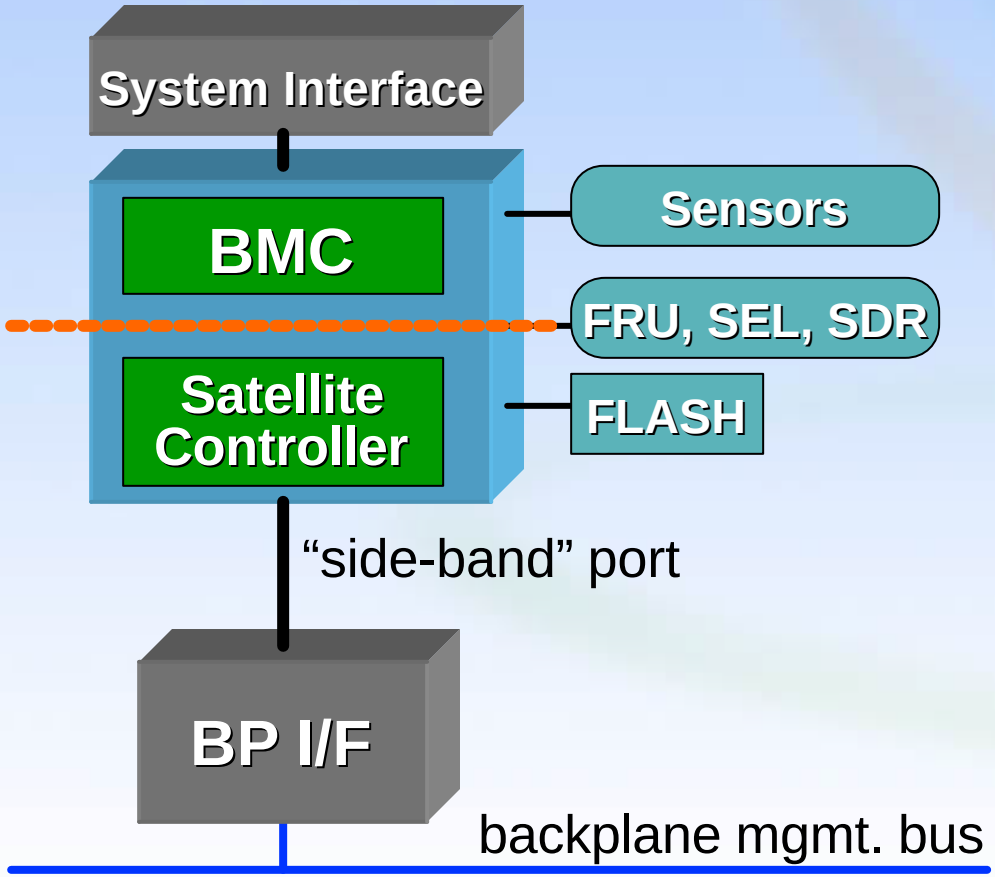
Firmware Firewall

Partitioning for protection

- **Problem: Bus topology enables local mgmt s/w to access other nodes**
- **Solution: "firmware firewall"**



Firmware Firewall



- F/W blocks messaging to other nodes on shared bus
- Allows messages between local software and management module
- Local software may also be blocked from SDR or FRU updates that might be used to generate false events
- Firmware updates can only occur from management bus side
- Access rights can only be configured from management bus side

Firmware Firewall

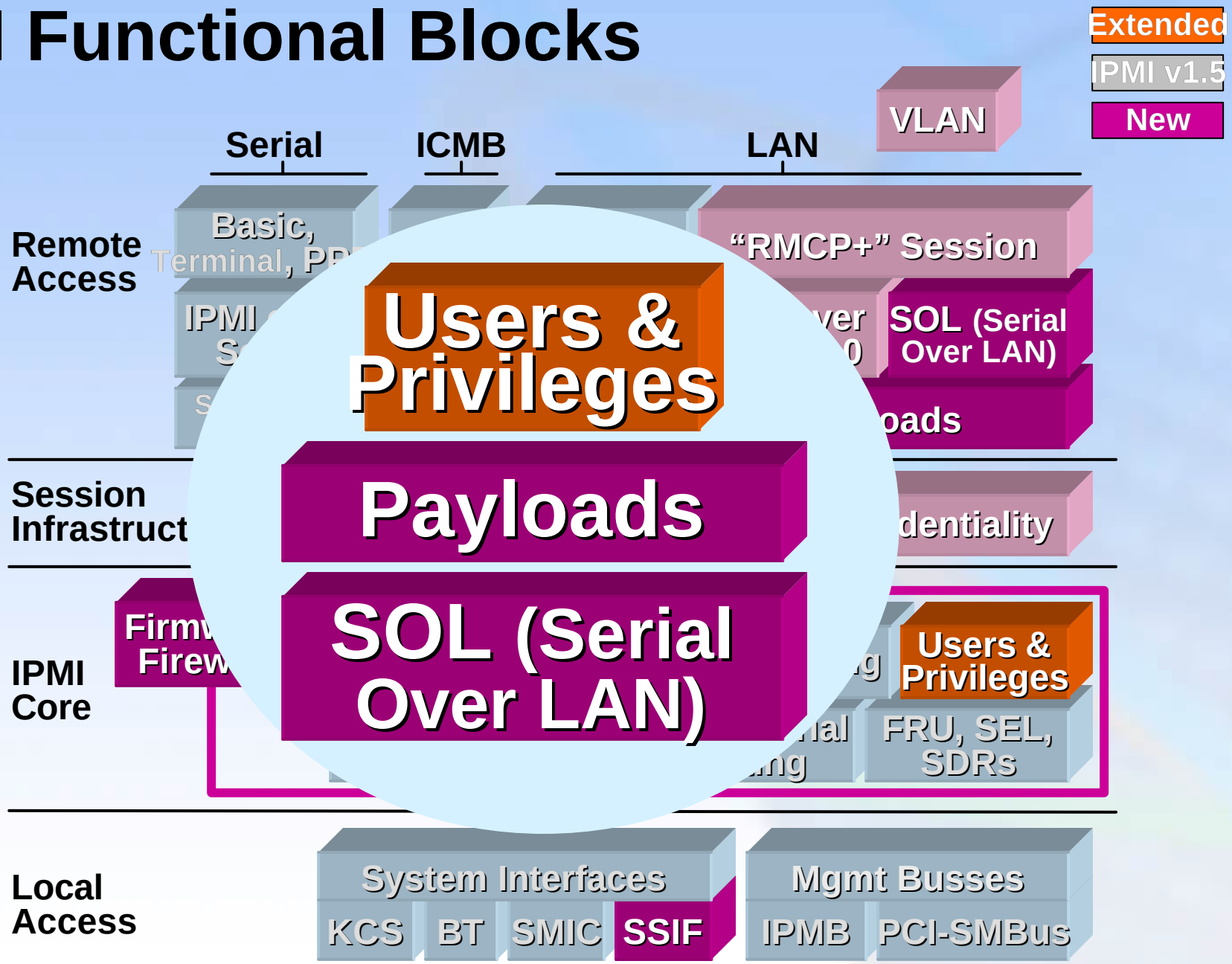
- ***Configurable Command Discovery*** **commands**
  - **Support discovering which commands and sub-functions can be enabled/disabled**
  - **Two commands:** ***Get Configurable Commands, Get Configurable Command Sub-functions***
- ***Command Configuration*** **commands**
  - **Provide mechanism for enabling/disabling those commands**
  - **Four commands:** ***Set/Get Command Enables, Set/Get Command Sub-function Enables***

Firmware Firewall

Command Discovery commands

- Enable software to discover what commands and subfunctions are available on given mgmt. controller
- Discovery commands can be implemented separate from Firmware Firewall enable/disable commands
- Centralize command and sub-function discovery
  - Augments IPMI distributed parameter, and 'try command' discovery
  - Command and sub-function support can vary on a PER CHANNEL basis
- Three commands: *Get NetFn Support*, *Get Command Support*, *Get Command Sub-function Support*

IPMI Functional Blocks



Users & Privileges

- **Per Channel Multi-level, Multi-User Security**
  - **User, Operator, Admin and OEM Privilege levels for IPMI commands**
  - **Per-user configurable enables for payload access (e.g. SOL)**
- **IPMI v2.0 Login Options**
  - **'Anonymous' login: no username or password required**
    - Can be enabled for a given privilege level. E.g. "User Level"
  - **Role-based login: password only, no username, for a given privilege level**
    - E.g. "Admin" login
  - **Username login: user name and user password required**
  - **'Two key' login: user/role password plus 'BMC Key'**
    - Can prevent multiple system access by 'human engineering' a single username/password pair.

Flexible configuration enables security to be tailored to site needs

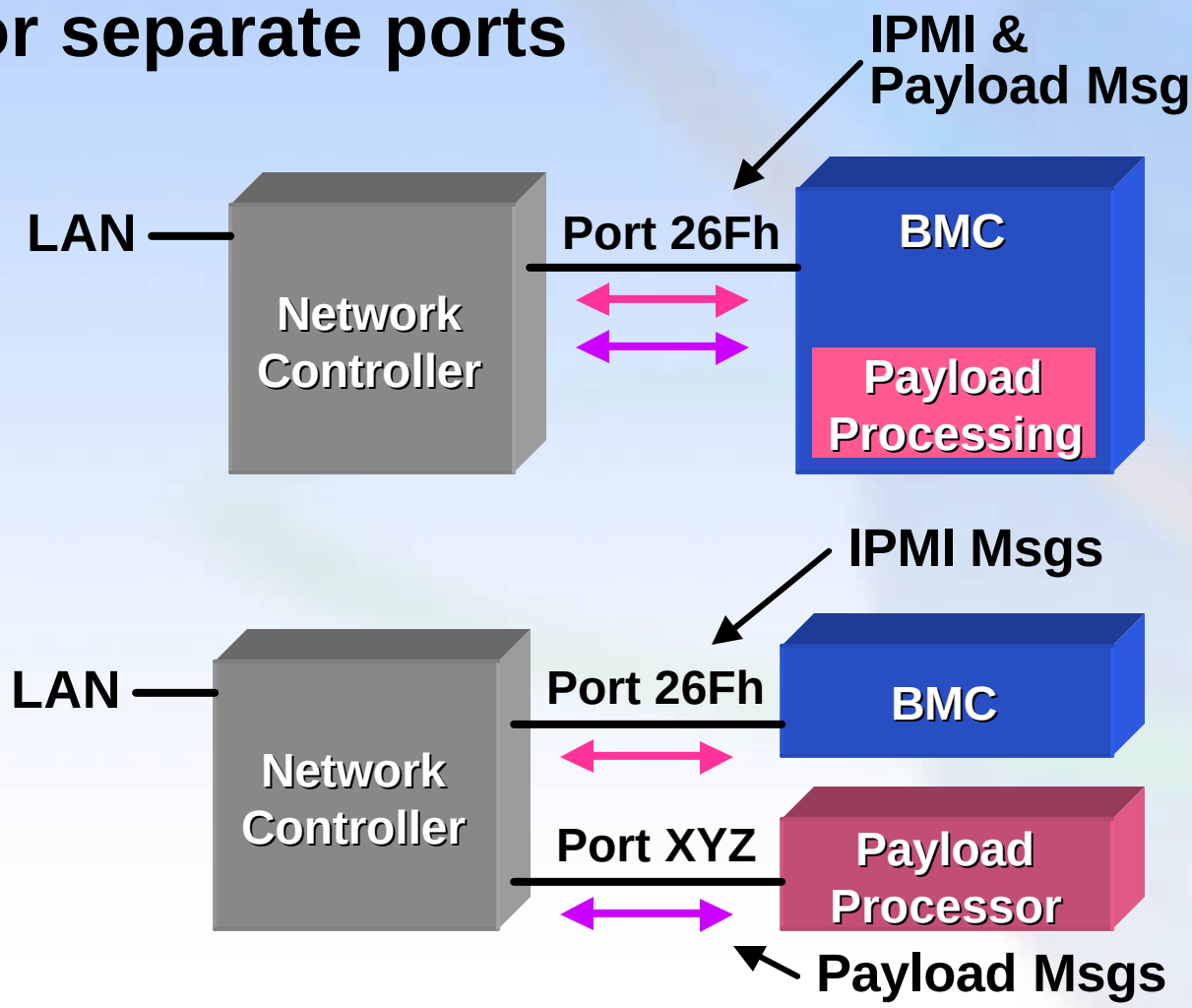
Payloads

- **Payloads enable multiple types of traffic to be carried over a single IPMI session**
  - **payloads can also be launched to a separate session**
- **Standard and OEM Payload Types supported**
  - **Standard payload types: Support Session Setup, IPMI Messages, "Serial Over LAN"**
  - **OEM payload types: Enable value-added features on IPMI session infrastructure (e.g. KVM)**
    - **Leverages IPMI User configuration and authentication**
- **Payload support is discoverable**
- **Payload access enabled on a per-user basis**

Session Payloads Enable "1-port" Management

Payloads

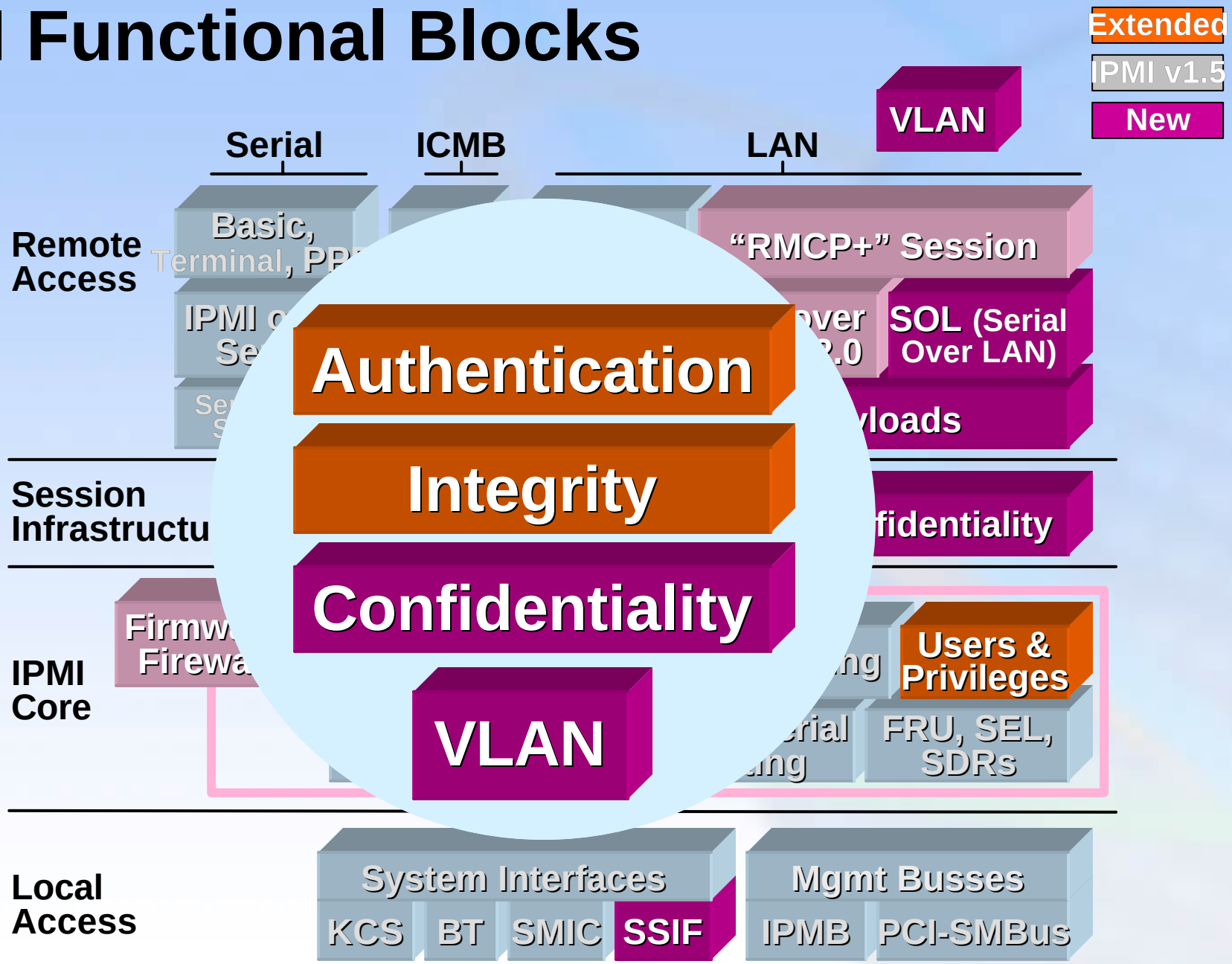
Payloads can be activated under common or separate ports



Serial Over LAN

- Defines common format and protocol for seria redirection under an IPMI Session
  - Redirects baseboard “16550” serial controller interface over LAN
  - Launched as a standard payload type under IPMI v2.0 Session
- Specification supports multiple serial connections
- Can be combined with IPMI Serial Port Sharing
  - Enables single ‘back of the box’ serial connection to be shared for local serial/modem, BMC access, and LAN redirected management

IPMI Functional Blocks



Authentication, Integrity, and Confidentiality

- **Authentication Algorithm:** Defines what steps are used for authenticating a User and establishing a session
  - **E.g. IPMI v2.0 uses for RAKP (remote access key exchange protocol)**
- **Integrity Algorithm:** Defines algorithm for signing packets after session has been established.
  - **E.g. HMAC-SHA1-96**
- **Confidentiality (encryption) Algorithm:** Defines algorithm for encrypted payload data in a session.
  - **E.g. AES-128 (Advanced Encryption Standard)**
- **Combination of Authentication, Integrity, and Encryption algorithms defines a CipherSuite**
- **Standard CipherSuites** provide algorithm to trade-off between strength and performance
- **OEM CipherSuites** also supported

Encrypted and Authenticated Packets

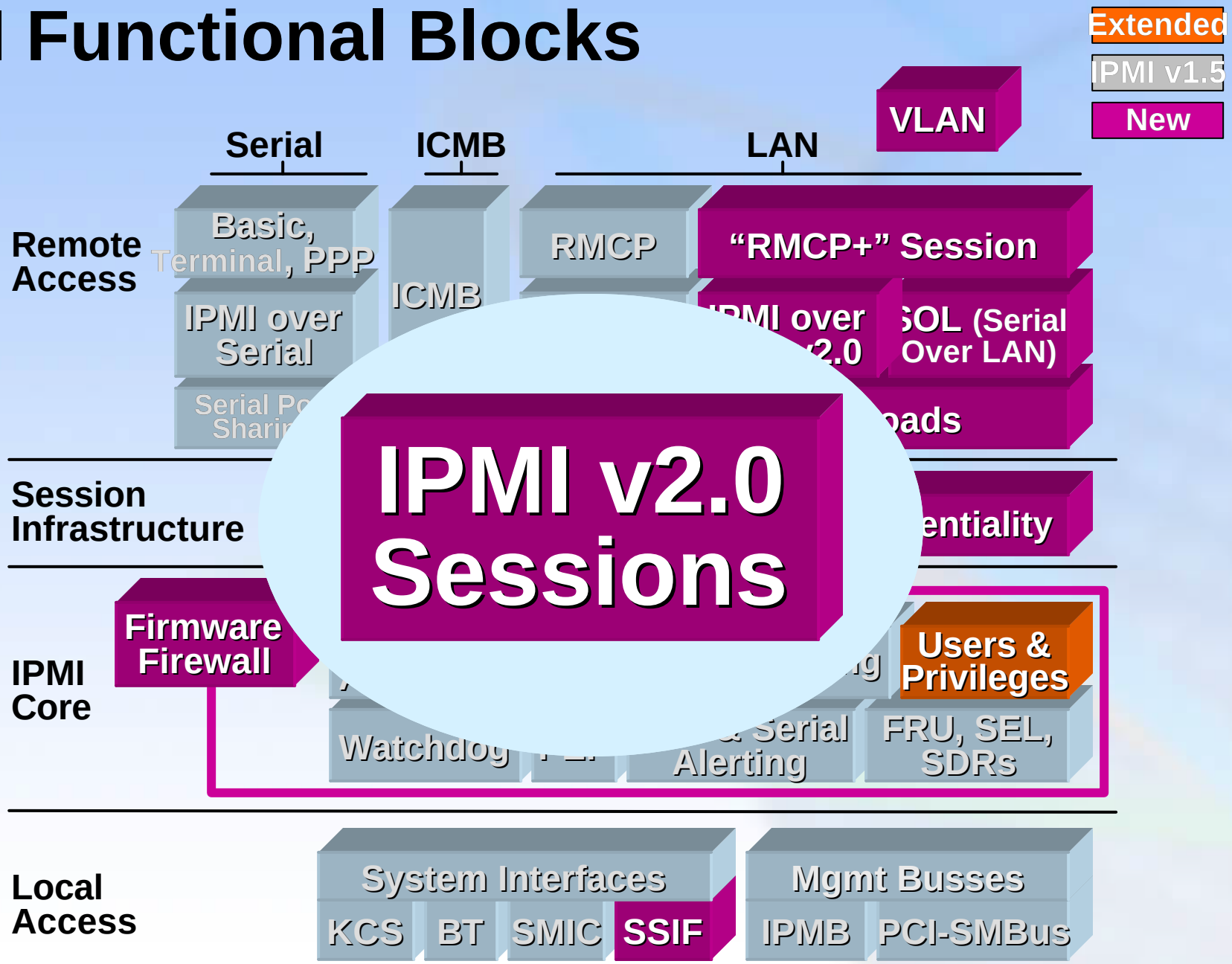
- **Authenticated / Unauthenticated and Encrypted / Unencrypted packets can be mixed in single session**
  - Improves performance on small micros. Bits in payload type field indicate whether the payload data is authenticated and /or encrypted
- **Remote console can be given option to control when payload data is encrypted**
  - Allows console to decide when an operation, e.g. remote password configuration, requires encryption
  - For IPMI messages, an encrypted request gets an encrypted response
  - For other payloads, a *Suspend/Resume Encryption* command is used
- **Can configure BMC to *require* that payload is encrypted.**
  - Prevents mis-behaved console from exposing sensitive data.

IPMI v2.0 technology reduces overhead for secure remote management

VLAN

- IPMI v2.0 LAN Packet format extended for “Virtual LAN” routing per IEEE 802.1q
- Works with side-band filtering in enhanced management network controllers
- VLAN support configurable on a per-channel basis

IPMI Functional Blocks



Sessions

Discovery and Connection

- **Enhanced User Login Options**
  - New option for ‘Role-only’ logins
  - Simplifies use in small installations
    - no username to remember, can simply login in as User, Operator, or Admin
- **New commands for managed system discovery**
  - Facilitates automated discovery and access by remote applications
  - IPMI version (v1.5 or v2.0) discovery
  - Cipher-Suite discovery
  - Available Payloads
  - Existence of Anonymous and One- or Two-key login
    - enables remote console to present appropriate username and password entry options

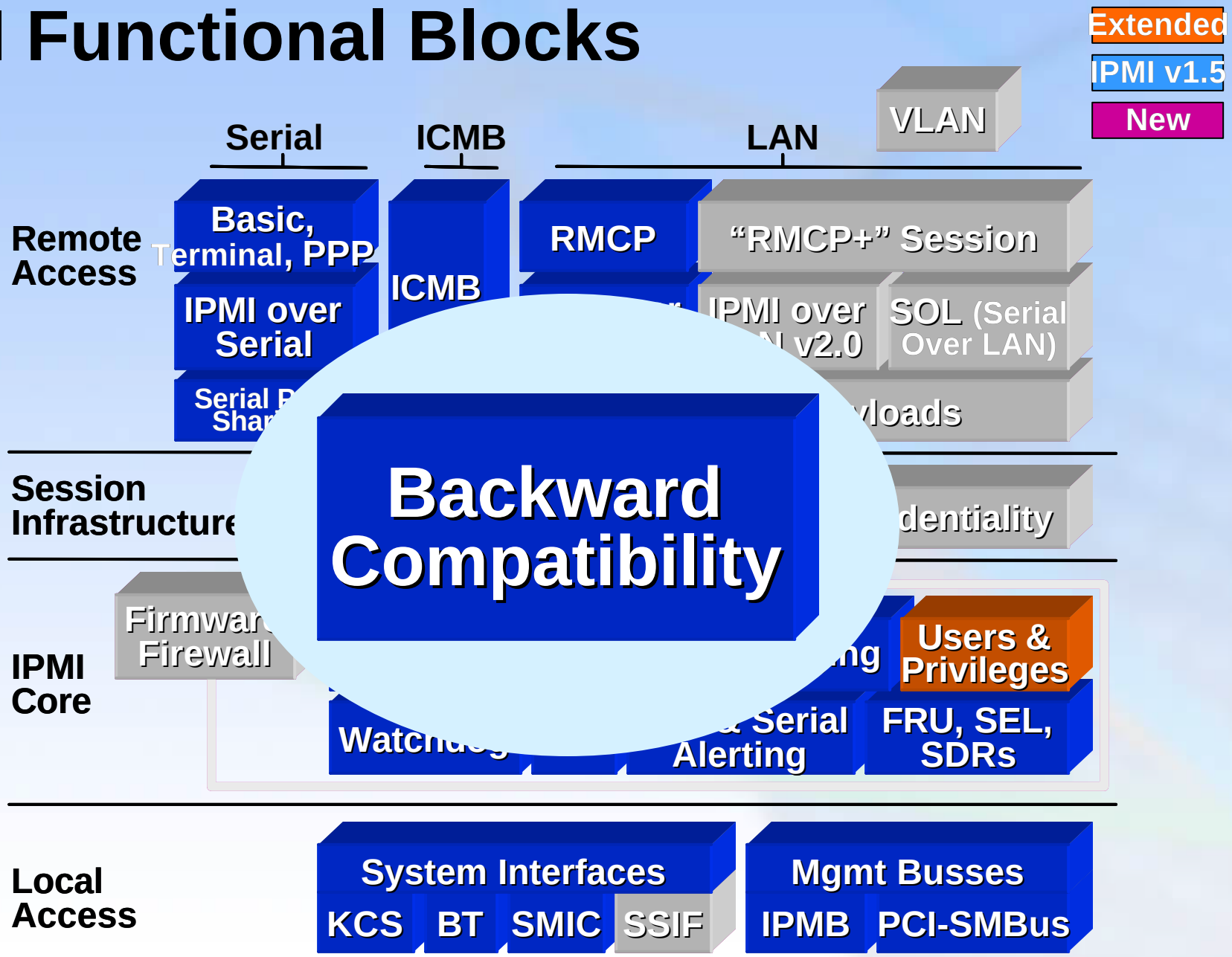
v2.0 Session Activation

- Discover IPMI support using *Get Channel Authentication Capabilities* command
  - Enables discovering IPMI version
  - Tells console whether 'anonymous' and/or '1-key' logins are enabled
  - Same command for v1.5 and v2.0
- Issue *Get Cipher Suites* command
  - Pick cipher suite for the maximum privilege level you want to establish the session at
- Activate session for given user…
  - IPMI v2.0 Uses dual Challenge/Response vs. IPMI v1.5 single challenge / response

v2.0 Session Activation

- Send *Open Session Request*
  Get *Open Session Response*
  - Sets session IDs and negotiates a ciphersuite
- Send *RAKP 1 Message*
  Get *RAKP 2 Message* as Response
  - Submits username and target privilege level to BMC
  - Exchanges random numbers between console and BMC
  - Roughly equivalent to the console submitting a challenge to the BMC and the BMC submitting a challenge to the console.
- Issue *RAKP 3 Message*, Get *RAKP 4 Message* as Response
  - BMC and Console exchanged 'signed' RAKP 3 and RAKP 4 packets
  - Signature based on the random numbers and key data associated with the user
  - Session is activated when both parties verify the signed packets.

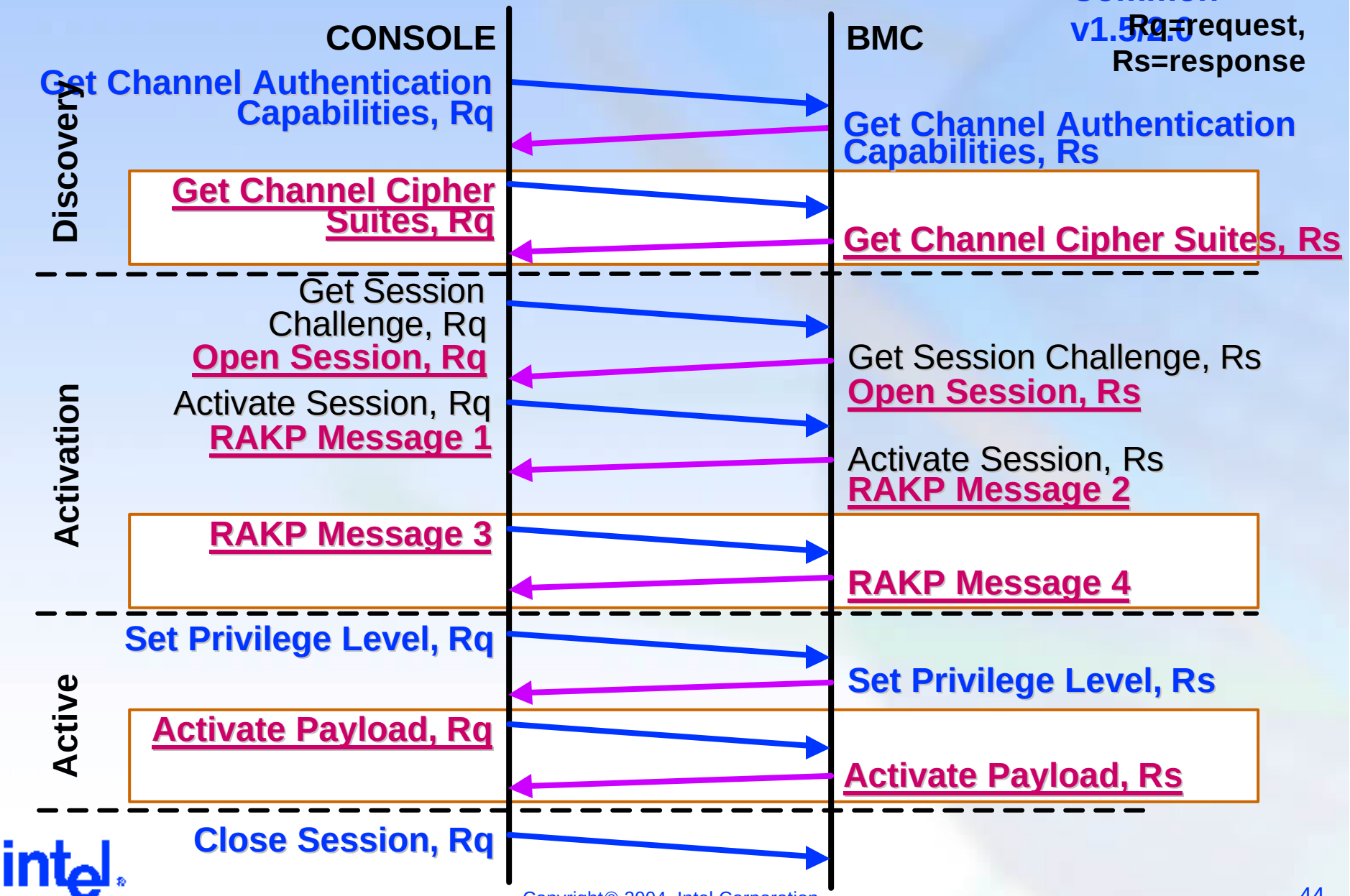
IPMI Functional Blocks



Backward Compatibility

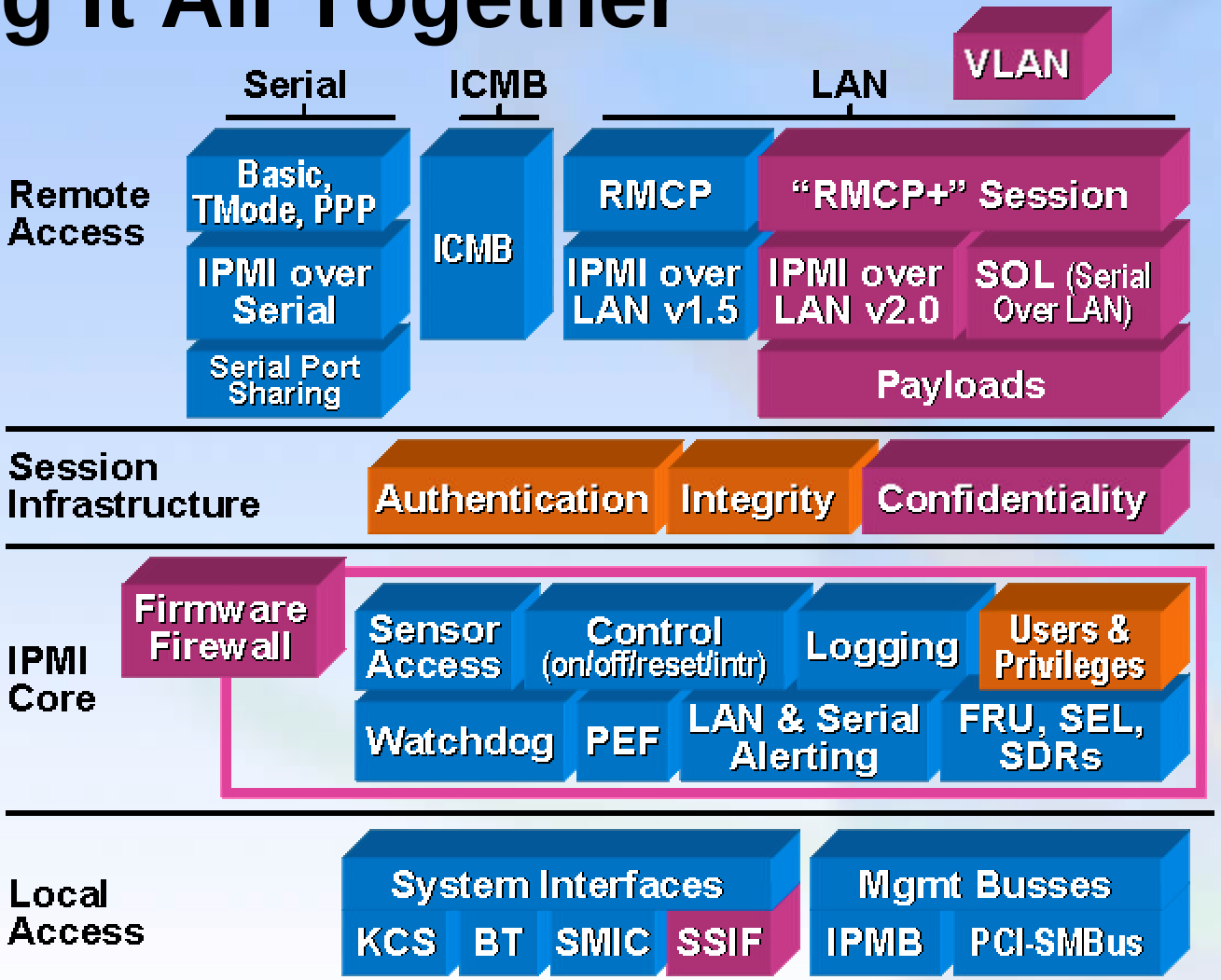
- Compatible command superset
  - Extends but does not replace IPMI v1.5 commands
- Managed systems can be discovered and used as an IPMI v1.5 system
  - Implementation can support both IPMI v2.0 and IPMI v1.5 connections simultaneously
  - Supports connecting using IPMI v1.5 protocols
    - IPMI v1.5 LAN packet support retained
- V2.0 packets/protocols required for new LAN features
  - e.g. enhanced auth., encryption, Serial Over LAN

IPMI Session Activation



Putting It All Together

Extended
IPMI v1.5
New



IPMI v2.0 technology enables secure remote management

Agenda

- IPMI Architecture and Initiative Update
- What's New in IPMI v2.0?
- IPMI v2.0 Technology: How IPMI v2.0 meets platform management needs
- IPMI in Action
- IPMI Futures

IPMI in HP's Integrity Servers


Integrity rx2600


Integrity rx4640


Integrity rx7620


Integrity rx8620


Integrity Superdome

- As one of IPMI's founding companies - HP has a long history of building industry standards around manageability.
- HP's entire line of Integrity IPF servers use IPMI, from the smallest 2-way server to the largest Superdome.
- HP uses IPMI, along with other manageability standards like WBEM, to build interfaces that promote interoperability between OS's and platforms.

IPMI is Highly Scalable

hp invent

Intel Developer Forum

HP: Enabling customer features

- IPMI fits well into the ecosystem of HP's value-added embedded management, covering some of the most basic functionality in a standard way
  - OS absent server health and server power control
  - Storage and retrieval of system event logs
  - A standard messaging mechanism for use with HP agents on Windows, HPUX, and Linux
- Upon this foundation, HP builds more features, to further enhance the manageability solution
  - Independent management LAN with secure (https) web interface or convenient Telnet UI to the management processor
  - Embedded web console
  - Enhanced event logging and diagnosis
  - Unique collaboration and repair features
  - Partition management, and more…

IPMI Supports Value Added Features

IPMI In Action

Dell Computer

"Standards simplify the computing environment and establish a common hardware and software platform, make it easier for systems to work together and to exchange information. Standards also simplify product development and service, thereby reducing our costs."

Michael Dell

- **Dell and IPMI**
  - Dell a founding IPMI Promoter
  - IPMI a core management technology for today's Dell PowerEdge servers
- **IPMI benefits for Dell Customers**
  - Helps lower server acquisition, training and operations costs
  - Enhances server availability
  - Enables server management with common tools and processes
- **IPMI 2.0 extends these benefits**
  - Enhances IPMI management security
  - Extends administrators reach with serial-over-LAN operations
  - Demonstrates industry focus on driving management standards

IPMI Delivers Common Management Interfaces

IPMI In Action

Dell PowerEdge™ 3250:

An IPMI Manageable Standards-Based Server

A cost effective, scalable solution for compute intensive applications utilizing Itanium Processor Family and standards-based manageability

- **Standards-based manageability for high performance computing**
  - **IPMI 1.5 server management**
  - **SMART drive monitoring**
  - **DMTF SMBIOS and ASF alerting**
- **Pro-active management for the scalable enterprise**
  - **Centralized operations enabled with IPMI monitoring and alerting**
  - **Remote control and recovery functions through IPMI server control, remote consoling**
  - **Large-scale remote operations via IPMI command-line interface**

DELL **IPMI Supports "Real Server" Management** Intel Developer Forum

IPMI In Action

Intel Corporation

- One of the Founding Companies for IPMI
- Over 5 years of IPMI-based Management for Server Building Blocks
  - In pedestal, rack, and modular (blade) chassis
  - In Entry through Enterprise
  - With Itanium®, Xeon™, and IA-32 processors
  - In General Purpose and Telco systems
  - Small business to Data Center

IPMI Works Across System Classes

Intel Corporation

- Over 7 product generations
- Over 5 different processors used for BMCs
  - some large systems have had as many as four management controllers
- Use IPMI SDRs to tailor server building blocks to customer
- Implementations take advantage of Intel processor and chipset management features
  - E.g. Memory and Bus Correctable and Uncorrectable error status, power state information, temperature and throttling status, etc.

IPMI Is Proven Technology

- Abit Computer Corp.
- Acer Inc.
- Adtron
- Amphus Inc.
- Advanced Micro Devices, Inc
- Agilent Technologies GmbH
- Alberta Microelectronics
- Allion Computer Inc.
- American Megatrends Inc.
- Arima Computer Corp.
- Artesyn Communication Products, Inc.
- ASIS LTD.
- ASUSTek Computer, Inc.
- Aventail Corporation
- Avian Communications
- Avocent, Inc.
- Axil Computer, Inc.
- Blue Wave Systems
- Bull S.A.
- C&D Technologies, Inc.
- California Digital Corp.
- Celestica
- C-MAC Engineering
- ColoWATCH, Inc
- Communication Automation Corporation
- Compellent Technologies, Inc.
- Concurrent Technologies, PLC
- CyberGuard Corporation
- Cyclades Corporation
- Data General Corporation
- Decru, Inc.
- Dell Computer Corporation
- Demac Associates
- Digi International
- Egenera, Inc.
- ElanVital Corporation
- Ericsson UAB
- ESO Technologies
- Evans & Sutherland
- Eversys Corporation
- Exabyte Corporation
- Extreme Engineering Solutions, Inc.
- Fabric7 Systems, Inc.
- First International Computer, Inc.
- FORCE Computers GmbH
- Forward Technologies
- Flextel SpA
- Freedom Technologies Corp.
- FreeIPMI Core Team
- Fujitsu, Ltd.
- Fujitsu Siemens Computers
- GoAhead Software, Inc.
- Gluon Networks, Inc
- HADCO Corporation
- HCL Infosystems Ltd.
- Hewlett-Packard Company
- Hewlett-Packard GmbH
- Hitachi Ltd.
- Hybricon Corporation
- IBM
- Ibus/Phoenix Corporation
- InnoMediaLogic, Inc.
- Integra Micro Sys. (P) Ltd.
- Intel Corporation
- Interphase Corporation
- InterWorks Computer Products
- Inventec Corporation
- Ipex ITG
- JMC Products
- Kealia, Inc
- Kaparel Corporation
- L-3 Communications Corp.
- LANDesk Software
- LANTRONIX
- Legend (Beijing) Limited
- LeoStream Corp.
- Linux NetworX, Inc.
- Lynux Works, Inc.
- Macrolink, Inc.
- Magnetek, Inc.
- MEGWARE Computer GmbH
- Mercury Computer Systems, Inc.
- Micro-Star International
- Mirapoint, Inc.
- MiTAC International Corp.
- Mitsubishi Electric Corp. Info. Systems Engineering Ctr.
- Motorola Computer Group
- National Semiconductor Corp.
- NEC Corporation
- Nematron Corporation Network Appliance, Inc.
- Network Engines, Inc.
- Network Storage Solutions, Inc.
- NEWISYS, Inc.
- NOCpulse, Inc.
- OliData S.p.A.
- Olivetti Computers Worldwide
- OSA Technologies
- Open Source Development Lab
- PEP Modular Computers
- Performance Technologies, Inc.
- PetaStream Inc.
- PFU Limited
- Phoenix Technologies Ltd.
- Pigeon Point Systems
- Pinnacle Data Systems, Inc.
- Praim, Inc.
- Qlogic Corporation
- Quanta Computer Inc.
- Radisys Corporation
- RADVISION
- RAMIX Inc.
- Raritan Computer, Inc.
- Reliance Computer Corp.
- Samsung Electronics Co., Inc.
- Sanera Systems, Inc.
- SANgate Systems, Inc.
- Sanritz Automation Co., Ltd.
- SBS Technologies (Industrial Computers GmbH)
- Scenix Semiconductor, Inc.
- Siemens AG
- Silicon Graphics, Inc.
- SKY Computers, Inc.
- SMIS R&D, Inc.
- Snap Appliance
- Stan Cox and Associates
- Standard Microsystems Corp.
- Stratalight Communications, Inc.
- Stratus Computer Systems Ireland Ltd.
- Summit Microelectronics, Inc.
- Sun Microsystems
- Super Micro Computer, Inc.
- SyAM Software
- Symphony Group Intl. Co., Ltd.
- Synergy Microsystems
- Technobox, inc
- Teknor Applicom, Inc.
- T-Netix, Inc.
- Tatung Co.
- Tektronix
- Texas Micro Corporation
- Togabi Technologies, Inc.
- Toshiba Corporation
- Trilogic Systems, LLC
- Trimm Technologies
- Tyan Computer Corporation
- Universal Scientific Industrial Corp.
- USAR Systems, Inc.
- Vitesse Semiconductor Corp.
- Watrin System Design
- Wyselec
- VIA Technologies, Inc.
- Vividon, Inc.
- Vooha, Inc.
- Winbond Electronics Corp.
- WIPRO Infotech
- Xiotech Corporation
- Ziatech Corporation
- ZNYX Networks, Inc.

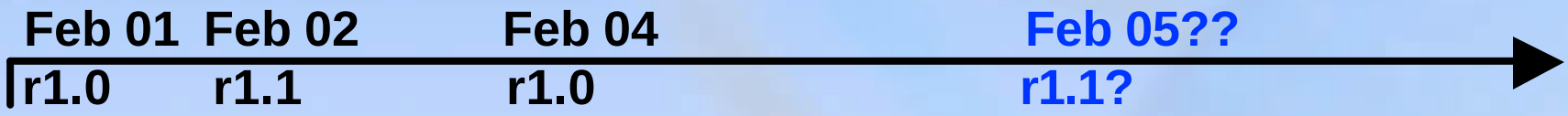
IPMI Technology is Widely Supported

Agenda

- IPMI Architecture and Initiative Update
- What's New in IPMI v2.0?
- IPMI v2.0 Technology: How IPMI v2.0 meets platform management needs
- IPMI in Action
- IPMI Futures

IPMI Futures

Advancing Platform Management



IPMI v1.5

- Monitoring (temp, volt, fan, etc.)
- Control (power on/off/cycle, reset, diag. interrupt)
- System Event Logging
- FRU & SDR Information
- Watchdog Timer
- Serial and LAN access
- Serial and LAN alerts
- Platform Event Filtering
- Serial Port Sharing
- Management busses

v2.0 Additions

- Session and Security Enhancements
- Serial Over LAN
- SSIF
- Alignment with ASF Authentication
- Encryption support
- Firmware Firewall
- Command Discovery
- Modular (blade) support

v2.0+ …

- New Payload Types
- Enh…
- …faces
- Links to Dire… based Authen…
- Impro… Group Control
- Auxili… og Acce…
- Integration with Web Interfaces
- Web services-based …

Proven Foundation for New Platform Management Features

New Capabilities Under Consideration

- Additional redirection payloads:
  - e.g. KVM, USB-media
- Improved configuration interfaces
  - Simplified save/restore of configuration settings
  - Secure migration of user configuration
  - Integration with configuration of 'Alternative Access' features, e.g. Web Server, Telnet
- Interfaces to Directory-based authentication
- More efficient options for 'group control'
  - E.g. option for 'persistent' connections

New Capabilities Under Consideration

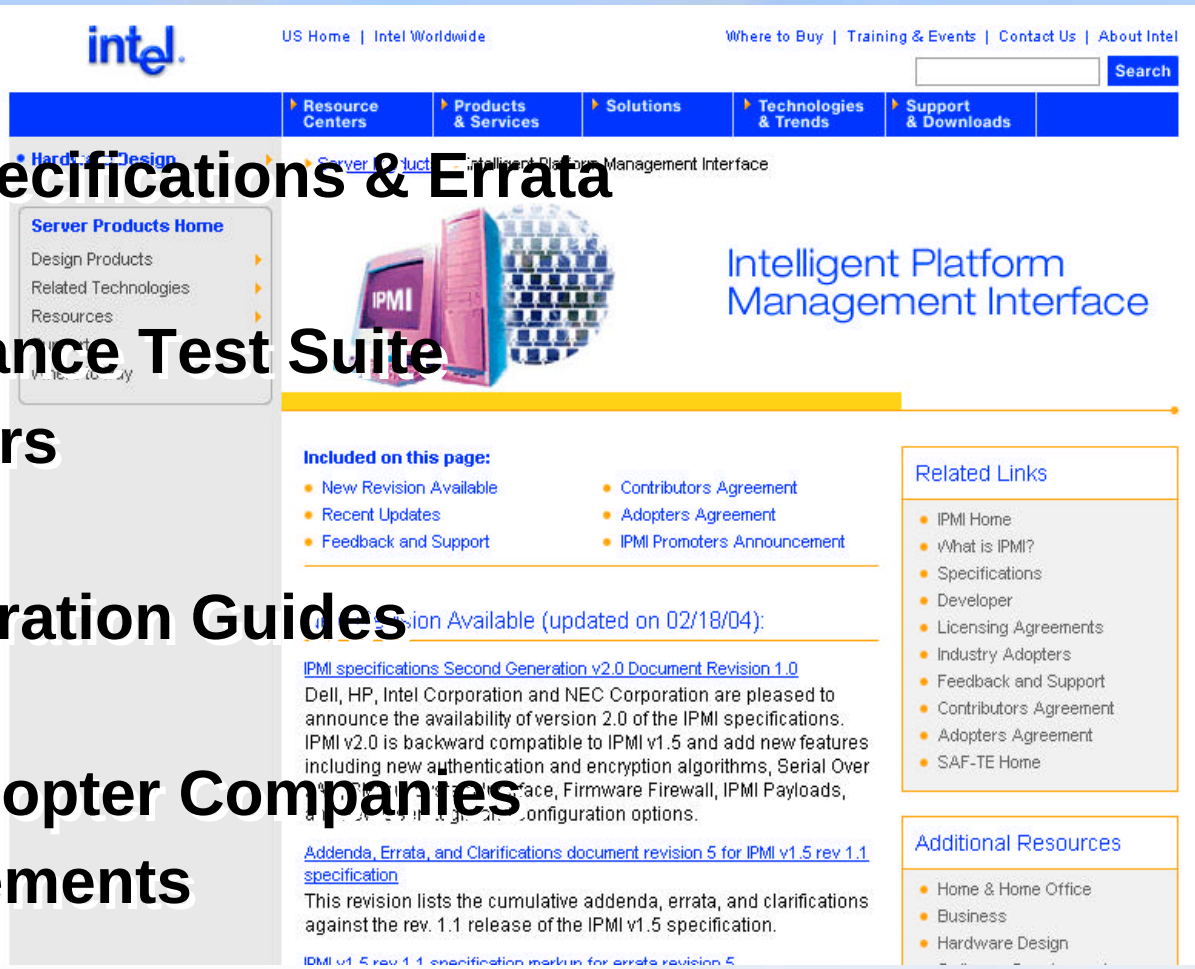
- Auxiliary Log access
- OOB configuration integration with web-based interfaces
  - enabling/disabling web server, CLI, Telnet
  - Configuring user privileges associated with secured interfaces
  - Integration with directory-based authentication
- Web-services –based interfaces
  - Alignment with “CIM+” / DMTF SMWG
  - “IPMI over XML/SOAP”

IPMI will continue to evolve with valuable new capabilities

Where to get More Info

IPMI Web Site

- Latest IPMI Specifications & Errata
- Presentations
- IPMI Conformance Test Suite
- Example Drivers
- Tools
- FAQ and Integration Guides
- Mailing List
- List of IPMI Adopter Companies
- Adopter Agreements



developer.intel.com/design/servers/ipmi

Summary

- IPMI reduces TTM and development cost for platform management
- IPMI v2.0 enables cross-platform manageability across server classes
- IPMI v2.0 technology enables secure remote management
- IPMI v2.0 technology is widely supported
- IPMI will continue to evolve with valuable new capabilities


Intel
Developer
Forum
intel

Backup Slides

SSIF - SMBus System Interface

Operation	SMBus CMD	SMBus Protocol
BMC Single Part Write	**0x02**	**Write Block**
BMC Multi-Part Write - Start – first part	**0x06**	**Write Block**
- Middle part(s) if any	**0x07**	**Write Block**
- End – last part	**0x08**	**Write Block**
BMC Single Part Read	**0x03**	**Read Block**
BMC Multi-Part Read - Start – first part	**0x03**	**Read Block**, first two data bytes after length = [0x01,0x00]
- Middle part(s) if any	**0x09**	**Read Block**, first data byte after length = 0x00
- End – last part	**0x09**	**Read Block**, first data byte after length = 0x01

IPMI Functional Blocks